EXHIBIT I

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation,

Plaintiff and
Counterclaim-Defendant,

v.

INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia Corporation, and SYMANTEC CORPORATION, a Delaware corporation,

Defendants and
Counterclaim- Plaintiffs.

Civil Action No. 04-CV-1199 (SLR)

SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11

Pursuant to Federal Rules of Civil Procedure 26 and 33, Defendant Symantec Corporation ("Symantec") supplements its responses to Plaintiff SRI International, Inc.'s ("SRI") Interrogatories Nos. 6 and 11.

GENERAL RESPONSES

1. Symantec's responses to SRI's First Set of Interrogatories are made to the best of Symantec's present knowledge, information and belief. Symantec's responses are subject to amendment and supplementation should future investigation indicate that amendment or supplementation is necessary. Symantec undertakes no obligation, however, to supplement or amend these responses other than as required by the Federal Rules of Civil Procedure and the Local Rules for the United States District Court for the District of Delaware.

2. Symantec's responses to SRI's First Set of Interrogatories are made according to information currently in Symantec's possession, custody and control.

3. To the extent that Symantec responds to SRI's First Set of Interrogatories by stating information that is private, business confidential, proprietary, trade secret or otherwise

protected from disclosure pursuant to Federal Rule of Civil Procedure 26(c)(7) or Federal Rule of Evidence 501. Symantec will respond pursuant to the terms of the Protective Order in this case.

4. Symantec reserves all objections or other questions as to the competency, relevance, materiality, privilege, or admissibility of any information, document or thing produced in response to SRI's Interrogatories as evidence in any subsequent proceeding or trial in this or any other action for any purpose whatsoever.

5. Symantec reserves the right to object on any ground at any time to additional interrogatories that SRI may propound involving or relating to the same subject matter as SRI's First Set of Interrogatories.

OBJECTIONS

Symantec incorporates the Objections contained in Symantec's Response to SRI's First Set of Interrogatories. The applicable foregoing general objections are incorporated into each of the specific objections and responses that follow. The stating of a specific objection or response shall not be construed as a waiver of Symantec's general objections.

SECOND SUPPLEMENTAL RESPONSES TO PLAINTIFF'S INTERROGATORIES NOS. 6 AND 11

INTERROGATORY NO. 6:

If you contend that any claim of any of the Patents-in-Suit is invalid, identify the specific statutory bases for the invalidity (e.g., 35 U.S .C. § 102(a)), the factual bases for that contention, any allegedly invalidating prior art or publications, where each element of the claim is found in the prior art or publications, and the three people most knowledgeable about the factual bases for your contention. Your response may take the form of a claim chart.

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 6:

Symantec objects to Interrogatory No. 6 to the extent that it requests the "three people most knowledgeable about the factual bases for your contentions." This portion of the interrogatory seeks the premature identification of the expert witnesses upon which Symantec intends to rely. Symantec further objects that this Interrogatory is overbroad to the extent that it requests information regarding claims that SRI has not asserted against Symantec in this litigation. SRI provided Symantec with a list of claims-at-issue in the Sept. 27, 2005 letter from Gina M. Steele to Jonathan D. Loeb. Symantec's responses are limited to the claims listed in that letter.[1] To the extent that SRI may later try to assert additional claims against Symantec, such action by SRI would be highly prejudicial to Symantec. Symantec reserves the right to supplement or modify these responses should SRI belatedly add claims.

[1] SRI's Sept. 27, 2005 letter stated: "Interrogatory No. 1. With regard to your request for the claims SRI is asserting against Symantec, SRI states as follows: SRI asserts that Symantec has infringed claims 1-23 of the '615 patent; claims 1-18, and 20-24 of the '212 patent; claims 1-5, 8-16, 18-22 of the '203 patent; and claims 1, 4, 11-18, 21 and 24 of the '338 patent." These claims will be referred to herein as "the claims-at-issue."

Moreover, despite repeated requests, SRI has not provided specific contentions regarding the conception date(s) for the alleged "inventions" claimed in the patents-in-suit. Instead, SRI has provided an approximately one year date range for conception of the '338, '203, and '615 patents, and an approximately two year date range for conception of the '212 patent.[2] SRI's failure to substantively respond to Symantec's Interrogatory No. 4, which requested the date(s) of conception and reduction-to-practice for each alleged "invention" claimed in the patents-in-suit, has severely prejudiced Symantec. Consequently, the patentability of the claims-at-issue must be assessed in light of the state of the relevant art as of the filing date of the original application from which the patents issued. Symantec intends to present evidence at trial that establishes and broadly illustrates the state of the art in intrusion detection and network monitoring as of November 9, 1998. Symantec may rely upon publications, patents, percipient and expert testimony, and/or contemporaneous and predecessor products to reveal the state of such art at that time (or as of any earlier date if Plaintiff offers legally adequate proof of an earlier date of invention).

The information provided in Symantec's response is preliminary in nature and subject to modification and supplementation. For example, Symantec has only recently received limited documents from SRI relating to the development work that led to the patents-in-suit and certain prior art systems and references, which Symantec has begun to review. Symantec continues to develop and refine its understanding of the state of the art as additional relevant information is acquired during the course of ongoing discovery. Ongoing discovery efforts may identify

[2] *See* SRI International Inc.'s First Supplemental Response to Interrogatory Nos. 4-10 and 12 of Defendant Symantec Corporation's First Set of Interrogatories [Nos. 1-12], Supplemental Response to Interrogatory No. 4.

additional prior art references or embodiments that are relevant to the invalidity of the claims-in-suit. Symantec will supplement this response in a timely manner upon receipt of sufficient information relating to such additional prior art references or embodiments.

Symantec further objects that this interrogatory is premature because Symantec has not been provided with any understanding of SRI's proposed claim constructions, and therefore is unable to determine how SRI's proposed claim constructions inform the anticipation and obviousness contentions disclosed herein. Furthermore, the contentions set forth below are not based upon Symantec's proposed claim constructions. Symantec reserves the right to supplement and modify its invalidity contentions under 35 U.S.C. §§ 102 and 103 subject to the claim constructions advanced by SRI and Symantec pursuant to the Court's Scheduling Order, which specifies that "on January 20, 2006, the parties shall exchange lists of those claim terms that they believe need construction and their proposed claim construction of those terms" and that the "parties shall agree upon and file the Joint Claim Construction Statement on February 17, 2006, with the claim chart separately docketed." The complete scope of available prior art and its applicability to individual claims-at-issue will not be certain until the Court has construed the claims of the patents-in-suit. Symantec therefore further reserves the right to supplement and modify these contentions once the Court has construed the claims.

The accompanying prior art charts, attached hereto as Exhibits A-1 – A-23, reflect Symantec's current understanding of the primary prior art references and embodiments upon which it intends to rely to establish anticipation of the claims-in-suit under 35 U.S.C. § 102 and/or obviousness under 35 U.S.C. § 103. To the extent that a particular prior art reference or embodiment does not alone anticipate all the limitations of any one of the claims-in-suit as ultimately construed by the court, Symantec reserves the right to combine the references and/or embodiments disclosed herein with other references and/or embodiments that may complement any such reference or embodiment, to the extent that one skilled in the art at the relevant point in time would have had motivation to create such a combination.

Moreover, due to the extremely large number of prior art references that invalidate the claims at issue, as well as SRI's failure to provide conception and reduction-to-practice dates, Symantec cannot possibly list every combination of art that renders the claims-at-issue invalid under 35 U.S.C. § 103, and reserves the right to present different combinations of references and/or embodiments, to the extent that one skilled in the art at the relevant point in time would have had motivation to create such a combination.

Relevant Prior Art References Identified To Date

The knowledge of one skilled in the art as of Nov. 9, 1998 would have been informed by access to and appreciation of at least the following practices, publications, patents, and publicly available technologies, products, and systems. Symantec intends to rely upon these and similar references to establish the state of the anomaly detection, intrusion detection, network monitoring, and related arts prior to Nov. 9, 1998, and to establish that the claims-in-suit were anticipated under 35 U.S.C. § 102 or would have been obvious under 35 U.S.C. § 103 as of Nov. 9, 1998:

- All prior art of record in the file histories of the patents-in-suit; or identified in the Background of the Invention section of the patents-in-suit;
- All prior art references identified in Exhibits A-1 – A-23 attached hereto; and
- All prior art references produced to SRI at Bates ranges SYM_P_0067248 – SYM_P_0082525 and SYM_P_0498070 – SYM_P_0511901.

Additional Technologies, Products and Systems

- Argus,

- Arpwatch,
- ASIM (Automated Security Incident Measurement),
- Berkeley Packet Filter,
- Borderguard,
- Bro,
- Cabletron's Spectrum,
- CIDF (Common Intrusion Detection Framework),
- Computer Associates Unicenter TNG,
- CSM (Cooperating Security Managers),
- DIDS (Distributed Intrusion Detection System),
- EMERALD,
- FireWall-1,
- GrIDS (Graph based Intrusion Detection System),
- Harris Corporation Stake Out,
- Haystack,
- HP OpenView, Network Node Manager, and NetMetrix,
- IDES,
- Internet standards,
- IP Filter,
- ISM (Internetwork Security Manager),
- Ji-Nao,
- Libpcap,
- MIDAS (Multics Intrusion Detection and Alerting System),
- NADIR (Network Anomaly Detection and Intrusion Reporter),
- NetRanger,
- NFR (Network Flight Recorder),
- NIDES,
- NIDX,
- NSM (Network Security Monitor),
- Raxco AUDIT,
- Stalker, NetStalker and WebStalker,
- Sun Network Management System (Solstice Site Manager, Solstice Domain Manager, Solstice Enterprise Manager, and Sun Net Manager),
- Tcpdump,
- TCP Wrapper,
- TIS Firewall Toolkit,
- Tivoli Enterprise Manager, and
- Wisdom & Sense.

PRIOR ART REFERENCES THAT ANTICIPATE THE ASSERTED CLAIMS-AT-ISSUE

The prior art cited herein invalidates the claims at issue under 35 U.S.C. §102, as set forth in detail in the representative charts attached as Exhibits A-1 – A-22 to this Supplemental Response. The cover page of each chart provides citations to referenced prior art, as well as citations to related prior art disclosures. Representative anticipatory references include:

- Exhibit A-1: "Emerald 1997" and the additional references listed on page 1 of Exhibit A-1;
- Exhibit A-2: "Emerald - CMAD" and the additional references listed on pages 1-2 of Exhibit A-2;
- Exhibit A-3: "Emerald - Conceptual Overview" and the additional references listed on pages 1-2 of Exhibit A-3;
- Exhibit A-4: "Emerald - Conceptual Design 1997" and the additional references listed on pages 1-2 of Exhibit A-4;
- Exhibit A-5: "Emerald - Live Traffic Analysis" and the additional references listed on page 1 of Exhibit A-5;
- Exhibit A-6: "Network NIDES" and the additional references listed on page 1 of Exhibit A-6;
- Exhibit A-7: "Ji-Nao" (includes "Ji-Nao" and "Ji-Nao slides") and the additional references listed on page 1 of Exhibit A-7;
- Exhibit A-8: "NSM" and the additional references listed on page 1 of Exhibit A-8;
- Exhibit A-9: "DIDS February 1991 and DIDS October 1991" and the additional references listed on pages 1-2 of Exhibit A-9;
- Exhibit A-10: "GrIDS 1996 and GrIDS 1997" and the additional references listed on page 1 of Exhibit A-10;
- Exhibit A-11: "NetRanger" (includes "NetRanger User Guide 1.3.1" and "NetRanger product") and the additional references listed on pages 1-2 of Exhibit A-11;
- Exhibit A-12: "RealSecure" and the additional references listed on page 1 of Exhibit A-12;
- Exhibit A-13: "Network Level Intrusion Detection;"
- Exhibit A-14: "U.S. Pat. No. 5,825,750" and the additional reference listed on page 1 of Exhibit A-14;
- Exhibit A-15: "Fault Detection in an Ethernet Network via anomaly detectors" and the additional references listed on page 1 of Exhibit A-15;

- Exhibit A-16: "Stake Out Network Surveillance" and the additional reference listed on page 1 of Exhibit A-16;
- Exhibit A-17: "HP OpenView" and the additional references listed on pages 1-2 of Exhibit A-17;
- Exhibit A-18: "ISM" and the additional reference listed on page 1 of Exhibit A-18;
- Exhibit A-19: "Emerald 1997, Intrusive Activity 1991, NIDES 1994;"
- Exhibit A-20: Netstalker and HP OpenView" and the additional references listed on page 2 of Exhibit A-20;
- Exhibit A-21: "Network Flight Recorder" and the additional references listed on pages 1-2 of Exhibit A-21; AND
- Exhibit A-22: "AIS."

Citations to particular pages of a prior art reference in the attached prior art charts are to be understood as exemplary. Other pages of a prior art reference may also be relevant to the existence of a claim element, and Symantec reserves its right to supplement the page citations provided, if necessary. Symantec further reserves the right to supplement its § 102 contentions with additional prior art references because Symantec's investigation is still preliminary.

PRIOR ART REFERENCES THAT RENDER THE CLAIMS-AT-ISSUE OBVIOUS

In addition to anticipating the claims- at-issue, a very large number of combinations of the prior art references identified render some or all of the claims–at–issue obvious under 35 U.S.C. § 103. Representative examples of invalidating combinations of the prior art references are identified below. Symantec reserves the right to establish that any alleged "invention" claimed in the patents-in-suit would have been obvious and thus invalid under 35 U.S.C. § 103 based upon any combination of references identified herein, or similar to those identified herein, that one skilled in the art as of Nov. 9, 1998 would have had motivation to create.

- Exhibit A-2: "Emerald - CMAD" (for indicated claims);
- Exhibit A-3: "Emerald - Conceptual Overview" (for indicated claims);
- Exhibit A-4: "Emerald - Conceptual Design 1997" (for indicated claims);
- Exhibit A-17: "HP OpenView" (see page 2 of Exhibit A-17 regarding § 103 combinations);
- Exhibit A-18: "ISM" (see page 1 of Exhibit A-18 regarding § 103 combinations);
- Exhibit A-19: "Emerald 1997, Intrusive Activity 1991, NIDES 1994" (see page 1 of Exhibit A-19 regarding § 103 combinations);
- Exhibit A-20: "NetStalker and HP OpenView" (see page 2 of Exhibit A-20 regarding § 103 combinations);
- Exhibit A-21: "Network Flight Recorder" (for indicated claims);
- Exhibit A-23: Summary chart of other relevant prior art, listing, for each individual limitation of each claim-at-issue, the prior art references that satisfy each limitation and could be combined with any of the references listed in Exhibits A-1 – A-22.

Symantec has provided as Exhibit A-23 a chart indicating prior art references disclosing particular limitations of each claim-at-issue. Given the large number of combinations, Symantec cannot identify all of the possible permutations at this time. For each of the prior art charts listed above for anticipation and/or obviousness, any missing claims or limitations could be satisfied by combining the cited reference of the prior art chart with reference(s) from Exhibit A-23. Symantec reserves the right to combine the cited references in any combination or permutation that one of skill in the art as of Nov. 9, 1998 would have had motivation to create or evaluate. Symantec further reserves the right to supplement its § 103 contentions with additional prior art references because Symantec's investigation is still preliminary.

THE CLAIMS-AT-ISSUE ARE INVALID PURSUANT TO 35 U.S.C. § 112

The claims-at-issue are also invalid for failure to satisfy the best mode requirement under 35 U.S.C. § 112. SRI submitted source code in an Appendix to the patents-in-suit. A preliminary examination of the source code provided in the Appendix indicates that the code in the Appendix is not the complete program that existed at the time. For example, the Appendix code would not compile and run. In addition, the Appendix code contains no configuration files allowing for the use of any particular network traffic data categories. Furthermore, the Appendix code does not appear to have code for a resolver or an expert system. On information and belief, Symantec believes discovery will show that SRI had a more complete set of source code by the time it filed U.S. Patent Application No. 09/188,739 and withheld much of that code from the Patent Office. That withheld code reflected the inventors' best mode of practicing the claims-at-issue.

In addition, the patents-in-suit are invalid for failure to satisfy the enablement and written description requirements of 35 U.S.C. § 112. Furthermore, the claims-at-issue are invalid as indefinite because the claims fail to particularly point out and distinctly claim the subject matter of the invention.

Symantec's contentions regarding the invalidity of SRI's patents-in-suit pursuant to 35 U.S.C. § 112 are preliminary and subject to modification and review. For example, Symantec has not yet had the opportunity to depose either of the inventors. Furthermore, document production is still ongoing and Symantec has only begun its review of SRI's documents. In addition, despite Symantec's July 15, 2005 request for the production of SRI source code relevant to the patents-at-issue, SRI has not yet made any such source code available to Symantec.[3]

[3] *See* Symantec Corporation's First Set of Requests for Production of Documents to SRI International, Inc., RFP No. 31 (July 15, 2005).

INTERROGATORY NO. 11:

State all facts supporting your contention that the Patents-in-Suit are unenforceable by reason of SRI's alleged inequitable conduct.

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 11:

Symantec objects to this Interrogatory on the grounds that it is unduly burdensome because Symantec has already identified facts supporting its contentions regarding inequitable conduct in Symantec's Answer and Counterclaims to SRI International, Inc.'s First Amended Complaint filed on May 23, 2005. In addition, discovery has just begun in the case. Ongoing discovery efforts may identify additional facts showing the unenforceability of the patents-in-suit. Symantec will supplement this response in a timely manner upon receipt of additional relevant information. Subject to and without waiving the foregoing general and specific objections, Symantec responds by incorporating by reference paragraphs 40-41 of Symantec's Answer of May 23.

Symantec further responds with the following facts:

To the extent now known, and subject to further clarification as to the full extent of the withholding and misrepresentation of information, the inventors and/or their agents made a number of misrepresentations or omissions of material fact to the U.S. Patent Office, including but not limited to omissions regarding prior art.

"Network NIDES"

Intentional and material false statements or omissions were made by the inventors and/or their agents by the failure by applicants to disclose to the Examiner one of the inventor's own material prior art publications: *Next-generation Intrusion Detection Expert Systems (NIDES): A Summary*, by Debra Anderson, Thane Frivold, and Alfonso Valdes, SRI-CSL-95-07, May 1995 (hereinafter "*Network NIDES*"). In addition to the facts alleged in paragraphs 40-41 of Symantec's answer, the materiality of this reference is demonstrated by the "Network NIDES" chart at Exhibit A-6, which indicates that the reference anticipates most of the claims-at-issue. It is also demonstrated by SRI's submission of the Network NIDES reference to the PTO during the prosecution of pending patent applications, U.S. Patent Application Nos. 10/429,611 and 10/805,729, which are related to the patents-in-suit.

In addition, intentional and material false statements or omissions were made by the inventors and/or their agents by the failure by applicants to disclose to the Examiner several additional prior art publications with disclosures similar to the disclosure of *Network NIDES*:

- T. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, P.G. Neumann, and C. Jalali, *IDES: A Progress Report*, in Proceedings of the 6th Annual Computer Security Applications Conference, 1990 [SYM_P_0080629- SYM_P_0080641]. Relevant information from this publication includes, but is not limited to, the following:

> "8.5 Monitoring Network Traffic
> The theoretical basis for IDES can be extended so as to enable the development of an IDES that could monitor traffic in tactical communication networks to detect suspicious activity. The required extensions are twofold. … Second, IDES's rule base has been designed for detecting suspicious *user* activity. To use IDES to monitor network traffic, where user data are not available, we must create a rule base with a set of rules specific to the domain of detecting suspicious network traffic patterns.
> In addition to establishing the theoretical foundation for these two extensions to IDES, we would develop candidate architectures for incorporating one or more IDES into the network topology. So far IDES has assumed centralized control and is thus appropriate for systems with high channel capacity and low transfer delay. Tactical networks operating under stress are expected to have neither. Moreover, tactical networks can become partitioned, so that an IDES with centralized control would not have global knowledge. Thus, a distributed approach to detect anomalous behavior is more appropriate for tactical communications networks. We

> envision that IDES in this context would consist of a set of loosely coupled IDES machines." *Id.* at 283 [SYM_P_0080639].

- T.F. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, C. Jalali, H.S. Javitz, A. Valdes, and P.G. Neumann, *A Real-Time Intrusion-Detection Expert System (IDES)*, Interim Progress Report, Project 6784, SRI International, May 1990 [SYM_P_0078995- SYM_P_0079133].

Relevant information from the publication includes, but is not limited to, the following:

> "9.2.4 Monitoring Network Traffic
> The theoretical basis for IDES can be extended so as to enable the development of an IDES that could monitor traffic in tactical communication networks to detect suspicious activity. The required extensions are threefold.
> 1. IDES's statistical algorithms are based on the probabilities of occurrence of the events it observes. In a network, however, IDES would not be able to operate with global knowledge. Thus, IDES's algorithms must be extended to give meaningful results when some information is missing and probabilities can only be estimated.
> 2. IDES's rule base has been designed for detecting suspicious *user* activity. To use IDES to monitor network traffic, where user data are not available, we must create a rule base with a set of rules specific to the domain of detecting suspicious network traffic patterns.
> 3. IDES's statistical and rule-based components can be enhanced using ideas from visual pattern recognition theory, machine learning, neural networks (considered below), and other artificial intelligence techniques. This will enhance IDES's ability to make inferences about the type and location of suspicious activity by observing traffic.
> In addition to establishing the theoretical foundations for these three extensions to IDES, we would develop candidate architectures for incorporating one, or more, IDES into the network topology. So far IDES has assumed centralized control and is thus appropriate for systems with high channel capacity and low transfer delay. Tactical networks operating under stress are expected to have neither. Moreover, tactical networks can become partitioned, so that an IDES with centralized control would not have global knowledge. Thus, a distributed approach to detect anomalous behavior is more appropriate for tactical communications networks. We envision that IDES in this context would consist of a set of loosely coupled IDES machines." *Id.* at 82-83 [SYM_P_0079085 – SYM_P_0079086].

- T. F. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, P. G. Neumann, H. S. Javitz, A. Valdes, and T. D. Garvey, *A Real-Time Intrusion Detection Expert System (IDES) -- Final Technical Report*, Tech. Rep., SRI Computer Science Laboratory, SRI International, Menlo Park, CA, Feb. 1992 [SYM_P_0079206- SYM_P_0079370]. Relevant information from the publication includes, but is not limited to, the following:

> "Detecting Network Intrusions Current computing environments are, more and more, massively networked sets of workstations, servers, mainframes, supercomputers, and special-purpose machines and devices. Focusing on the vulnerabilities of any single host or even any single homogenous local network of machines may prove inadequate in such a distributed environment. Detecting intruders will require a comprehensive view of a network, possibly extending to other networks connected to the local network. Applying IDES technology to this (possibly heterogeneous) computing environment will require expanding the scope of IDES to include the ability to detect network intrusions as well as intrusions into the individual host machines. To achieve this, the following steps are necessary:
>
> - Build a rule base into IDES that contains specialized knowledge about network vulnerabilities and intrusion scenarios.
> - Enable IDES to work with partial information, since in a very large network it is unlikely that IDES will possess complete information about the whole network at all times. This capability will make IDES especially attractive for use in tactical communication networks, which must operate in hostile environments.
> - Develop an overall architecture for inserting IDES or a distributed set of component IDES machines into a large, complex network….
> - Network Intrusion Detection – We plan to develop and implement a capability for detecting network intrusions by combining a specialized rule base on network vulnerabilities with intrusion scenarios, develop a capability for the detection of intrusions with partial information, and develop an architecture for the integration of IDES into a large, complex network.
> - Large Network Architecture – We plan to develop an architecture for inserting IDES into a large network, and will we [sic] work with a U.S. Government installation (e.g., NOSC) to install IDES in such an environment." *Id.* at 95-97 [SYM_P_0079308 – SYM _P_0079310].
>
> "9.3 Monitoring Network Traffic

> We also plan to extend the theoretical basis for IDES to enable the development of an IDES that could monitor traffic in tactical communication networks to detect suspicious activity. The required extensions are twofold: …
>
> - IDES's rule base has been designed for detecting suspicious *user* activity. To use IDES to monitor network traffic, where user data are not available, we must create a rule base with a set of rules specific to the domain of detecting suspicious network traffic patterns.
>
> In addition to establishing the theoretical foundation for these extensions to IDES, we plan to develop candidate architectures for incorporating one or more IDES into the network topology. So far IDES has assumed centralized control and is thus appropriate for systems with high channel capacity and low transfer delay. Tactical networks operating under stress are expected to have neither. Moreover, tactical networks can become partitioned, so that an IDES with centralized control would not have global knowledge. Thus, a distributed approach to detect anomalous behavior is more appropriate for tactical communications networks. We envision that IDES in this context would consist of a set of loosely coupled IDES machines." *Id.* at 103-04 [SYM_P_0079316 – SYM_P_0079317].

In addition to failing to submit these references, SRI also failed to disclose to the Patent Office several § 102(b) references concerning the EMERALD project, the very project under which SRI performed the work that led to the filing of the patents-in-suit, as indicated by the referenced DARPA contract number in the specification of the patents-in-suit. These references include a paper for and presentation at the November 1996 CMAD Workshop ("Emerald – CMAD"), a Conceptual Overview paper, which was posted on SRI's website more than a year before the priority date of the patents-in-suit ("Emerald – Conceptual Overview"), and the Emerald Conceptual Design and Planning Document ("Emerald – Conceptual Design 1997"), which also was posted on SRI's website more than a year before the priority date of the patents-in-suit. The citations to these documents are found in the cover pages to Exhibits A-1 – A-4. The materiality of these references is demonstrated by the prior art invalidity charts attached as Exhibits A2 - A4. Moreover, much of the specification of the patents-in-suit can be traced to the disclosures in these references. All of these references were co-authored by one or more of the named inventors. Yet, none of them were cited to the Examiner.

The omitted *Network NIDES* reference, the three IDES references cited above, and the additional Emerald references cited above, would have been considered by a reasonable examiner to be material to a determination of patentability of the claims of the patents-in-suit, and on information and belief, said omissions were made with intent to deceive the U.S. Patent Office. Had the inventors and/or their agents made accurate representations to the U.S. Patent Office, the patents-in-suit would not have issued. Thus, the patents-in-suit are unenforceable for inequitable conduct.

"NSM"

In addition, intentional and material false statements or omissions were made by the inventors and/or their agents by the failure by applicants to disclose to the Examiner during prosecution of the '338 patent any publications regarding the Network Security Monitor ("NSM") including: L.T. Heberlein, G.V. Dias, K. N. Levitt, B. Mukherjee, J. Wood, D. Wolber., *A Network Security Monitor*, Proc. 1990 Symposium on Research in Security and Privacy, pp. 296-304, May 1990 [SYM_P_0068974 - SYM_P_0068956] and further including the additional references listed on page 1 of Exhibit A-8. The materiality of this reference is demonstrated by the "NSM" chart at Exhibit A-8, which indicates that the reference anticipates most of the claims-at-issue for the '338 patent.

The inventors were aware of the existence of the NSM system at least as early as May 1997. Phillip Porras was the co-author on a publication discussing NSM dated May 16, 1997, *see* [SRI012308-012404 at 012390].[4] In addition, P. Porras and P. Neumann, *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances*, 20th NISSC October 9, 1997 [SYM_P_0068831- SYM_P_0068843] states that "the Network Security Monitor [7] seeks to analyze packet data rather than conventional audit trails…" *id.* at [SYM_P_0068842].

The omitted *Network Security Monitor* May 1990 reference, as well as the related references listed on page one of Exhibit A-8, would have been considered by a reasonable examiner to be material to a determination of patentability of the '338 patent claims, and on information and belief, said omissions were made with intent to deceive the U.S. Patent Office. Had the inventors and/or their agents made accurate representations to the U.S. Patent Office, the '338 patent would not have issued. Thus, the '338 patent is unenforceable for inequitable conduct.

"Ji-Nao"

Intentional and material false statements or omissions were made by the inventors and/or their agents by the failure by applicants to disclose to the Examiner during prosecution of the patents-in-suit any publications regarding the Ji-Nao system, including:

- Y. Frank Jou et al., *Architecture Design of a Scalable Intrusion Detection System for the Emerging Network*, Technical Report CDRL A005, DARPA Order No. E296, Dept. of Computer Science North Carolina State University, April 1997 [SYM_P_0070541 – SYM_P_0070582].

[4] SRI has marked this document as "CONFIDENTIAL – Subject to Protective Order." However, the document itself indicates that it was publicly posted on the Internet at http://www.csl.sri.com/intrusion.html. Symantec believes this document has been improperly designated as Confidential. However, in an abundance of caution, Symantec has marked as Confidential Exhibit A-4, which provides the anticipatory disclosures of this document.

- Y. Frank Jou and S. Felix Wu, *Scalable Intrusion Detection for the Emerging Network Infrastructure*, IDS Program Review, SRI, July 1997 [SYM_P_0503679 – SYM_P_0503709].

These references, as well as the related references listed on page 1 of Exhibit A-7, would have been considered by a reasonable examiner to be material to a determination of patentability of the claims of the patents-in-suit. The materiality of these references is demonstrated by the "Ji-Nao" and "Ji-Nao slides" charts at Exhibit A-7, which indicates that both references anticipate the claims-at-issue of the patents-in-suit. The Ji-Nao system actually used the NIDES algorithms from SRI to perform statistical analysis: "the NIDES project at SRI is most extensive in its scope and development. It also has the most complete documentations available to the general public. With the understanding of statistical analysis's general applicability, we will adapt NIDES's statistical algorithm in our approach as a starting point and modify it as necessary." *See* Y. Frank Jou et al., *Architecture Design of a Scalable Intrusion Detection System for the Emerging Network*, Technical Report CDRL A005, DARPA Order No. E296, Dept. of Computer Science North Carolina State University, April 1997 at p. 18 [SYM_P_0070563].

The inventors were aware of the existence of the Ji-Nao system at least as early as November 1996. On information and belief, on November 12-14, 1996 at the CMAD IV Computer Misuse and Anomaly Detection Conference in Monterey, California, the inventors of the patents-in-suit presented the subject matter of the patents-in-suit during the same session as a presentation on the Ji-Nao system. During Session 4, Phillip Porras and Alfonso Valdes presented *Analysis and Response for Intrusion Detection in Large Networks*, a reference clearly related to the subject matter of the patents-in-suit because the conference summary discusses the

Emerald system on which the patents-in-suit are based and is an anticipatory reference, see Exhibit A-2. During this same session, Y. Frank Jou of MCNC presented *Scalable Intrusion Detection for the Emerging Network Infrastructure* [SYM_P_0500920 – SYM_P_0500969 at SYM_P_0500968]. *Scalable Intrusion Detection for the Emerging Network Infrastructure* was the title of multiple anticipatory references describing the Ji-Nao system, see Exhibit A-7.

Moreover, on information and belief, the named inventors were collaborating with Mr. Jou and his team. Mr. Porras prepared a December 16, 1996 quarterly report to Rome Laboratory, the governmental agency that was responsible for monitoring SRI's work under the DARPA contract for the EMERALD project, which references working with Mr. Jou of the Ji-Nao team. [SRI 11739-43].[5] In addition, Mr. Porras indicated in the May 20, 1997 *Conceptual Design and Planning for Emerald* document (see Exhibit A-4) that the Ji-Nao team at MCNC was using SRI's statistical profiler engine. [SRI 012308-12404 at SRI 012400[6]].

Furthermore, on information and belief, the Ji-Nao slides shown to be anticipatory in Exhibit A-7 were presented at SRI in July of 1997. *See* the Internet Archive of the MCNC website, listing the Ji-Nao slides as "Project Update Viewgraph (at SRI, July 97, powerpoint)" [SYM_P_0071957], see also [SYM_P_0499511 – SYM_P_0499601 at SYM_P_0499570].

In addition, on February 25-27, 1997, at the Intrusion Detection PI meeting in Savannah, Georgia Phillip Porras presented on SRI's Emerald system during the same day as Frank Jou of MCNC presented on the Ji-Nao system. *See* Feb. 21, 1997 email from Joe Daniero "re: tentative agenda for Intrusion Detection Meeting – Savannah" [SYM_P_0076782 – SYM_P_0076786 at

[5] SRI has marked this document "Confidential – Subject to Protective Order."

[6] Symantec believes SRI has improperly marked this document as Confidential. *See supra* note 4.

0076783].

In addition, correspondence from Phillip Porras regarding the Common Intrusion Detection Framework (CIDF) indicates that the Emerald team from SRI and the Ji-Nao team from MCNC and North Carolina State University worked closely together on the CIDF effort. *See* July 22, 1997 email from Phillip A. Porras to cidf@cs.ucdavis.edu entitled "A Common Intrusion-Detection Interface Specification Version 2.0 by Emerald/JiNao Groups (SRI, MCNC/NCSU)" [SYM_P_0500624 – SYM_P_0500639]. See also "The DARPA Common Intrusion Detection Framework – The CIDF Working Group" [SYM_P_0071467 – SYM_P_0071470].

The omitted Ji-Nao references would have been considered by a reasonable examiner to be material to a determination of patentability of the claims of the patents-in-suit, and on information and belief, said omissions were made with intent to deceive the U.S. Patent Office. Had the inventors and/or their agents made accurate representations to the U.S. Patent Office, the patents-in-suit would not have issued. Thus, the patents-in-suit are unenforceable for inequitable conduct.

Dated: November 15, 2005

DAY CASEBEER
MADRID & BATCHELDER LLP

By: Paul S. Grewal
Paul S. Grewal

Paul S. Grewal (*pro hac vice*)
Day Casebeer Madrid & Batchelder LLP
20300 Stevens Creek Blvd., Suite 400

Cupertino, CA 95014
Tel: (408) 873-0110
Fax: (408) 873-0220

Attorneys for Defendant and Counterclaim-Plaintiff Symantec Corporation

OF COUNSEL:

Lloyd R. Day, Jr. (*pro hac vice*)
Robert M. Galvin (*pro hac vice*)
Paul S. Grewal (*pro hac vice*)
Day Casebeer Madrid & Batchelder LLP
20300 Stevens Creek Blvd., Suite 400
Cupertino, CA 95014
Tel: (408) 873-0110
Fax: (408) 873-0220

Michael J. Schallop (*pro hac vice*)
Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
Tel: (408) 517-8000
Fax: (408) 517-8121

Dated: November 15, 2005